A Report
to the
Montana
Legislature

Information Systems Audit

Integrated Justice Information Sharing (IJIS) Broker

Department of Justice

April 2017

Legislative Audit
Division

15DP-05

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Members of the IS audit staff hold degrees in disciplines appropriate to the audit process.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Audit Staff

Aubrey J. Curtis
Diedra Murray

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Joe Murray

April 2017

The Legislative Audit Committee
of the Montana State Legislature:

This is our information systems (IS) audit of the Integrated Justice Information Sharing (IJIS) Broker managed by the Applications Services Division with the Montana Department of Justice.

This report provides the legislature information about general IS and application business process controls associated with the IJIS Broker and its corresponding data exchanges between the different justice agencies. This report includes recommendations for enhancing the timeliness and security of the data exchanges, as well as the disaster-recovery capability at the Department of Justice.

We wish to express our appreciation to the personnel from the Department of Justice for their cooperation and assistance during the audit, as well as those from the Department of Corrections and the Office of the Court Administrator who offered their time and expertise.

Respectfully submitted,

/s/ Angus Maciver

Angus Maciver
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

TABLE OF CONTENTS

Figures and Tables

Figures

Elected, Appointed, and Administrative Officials

Department of Justice Tim Fox, Attorney General

Mike Milburn, Chief of Staff

Liz Bangerter, Central Services Division Administrator

Joe Chapman, Justice Information Technology Services Division Administrator

Jack Marks, Applications Services Bureau Chief

Montana Legislative Audit Division

Information Systems Audit
Integrated Justice Information Sharing (IJIS) Broker
Department of Justice

April 2017 15DP-05 Report Summary

The IJIS Broker allows local, state, and federal agencies, as well as certain public entities, to share criminal justice information in a timely, accurate, and efficient manner. The expedient exchange of information is critical for justice agencies, most importantly law enforcement, to be able to carry out their mission and ensure public safety, including providing notifications for victims of violent crimes. The Department of Justice has made progress to date, but the full potential of IJIS Broker has yet to be achieved, due to the necessity of additional exchanges, upgrades to electronic criminal records, and an enterprise case management system for Montana courts (FullCourt). Based on the current status, crime victim notification through the IJIS Broker is inoperable at this time and may not be online when the Montana Constitutional Initiative 116, also known as Marsy's Law, takes effect in July 2017.

Context

The Department of Justice (DOJ) has pursued a number of grants to fund the IJIS Broker beginning in 2005 with the National Criminal History Improvement Program (NCHIP) grant of $269,000. Since its inception, DOJ has been awarded federal grants to help fund this system and is continuing to implement new exchanges and improvements. Crime Victim Notification through the IJIS Broker has been put on hold until an enterprise solution for the courts' case management system can be realized based on the need for a real-time interface to consistent court data.

Results

While the audit work focused on information system controls (general and application business-process) associated with IJIS Broker, the over-arching objective was to gain an understanding of the purpose of this system and whether it has accomplished what was intended. While the backbone infrastructure of the information sharing broker has been developed and deployed, there are data exchanges within the original project plan that have not yet been established. For the exchanges that do exist, the controls in place provide assurance that integrity of the data passed by the IJIS Broker is not compromised. The notifications of IJIS Broker should be re-examined to eliminate unauthorized disclosure of personally identifiable or criminal justice information. In addition, limitations with the current electronic criminal record repository (also known as Computerized Criminal History), as well as exchange partner business processes, present challenges to the timeliness of when information is shared with the justice community. Finally, the department can strengthen its continuity of operations capabilities in the case of a disaster or emergency to include an alternate "warm"

(continued on back)

site for the purpose of recovering critical information systems, including IJIS Broker, with the least amount of downtime.

Recommendation Concurrence	
Concur	6
Partially Concur	0
Do Not Concur	0

Source: Agency audit response included in final report.

For a complete copy of the report (15DP-05) or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to **lad@mt.gov**; or check the web site at **http://leg.mt.gov/audit**
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail **ladhotline@mt.gov**.

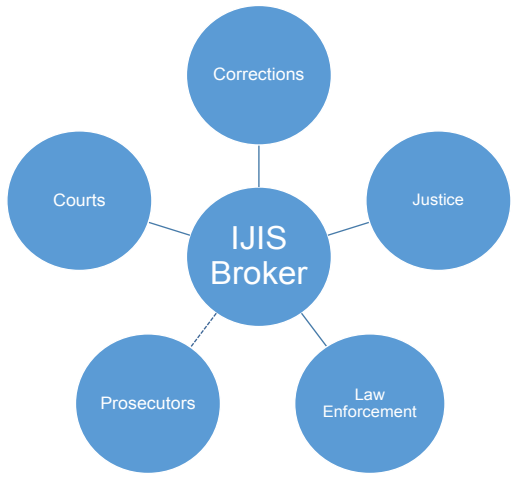
Chapter I – Introduction

Introduction

The concept of the Montana Integrated Justice Information Sharing (IJIS) Broker was conceived after the state was awarded the National Criminal History Improvement Program (NCHIP) grant in 2005 for $269,000. This, along with portions from other grants, funded the creation of the IJIS Broker and its initial exchanges. The expedient exchange of information is critical for justice agencies, most importantly law enforcement, to be able to carry out their mission and ensure public safety. The IJIS Broker does just this by facilitating accurate and timely information sharing among justice entities and the public. For instance, the driver information received by Montana Highway Patrol troopers in their cars, or updates on the status of an offender sent to a crime victim, would rely on the IJIS Broker to pass this data. A cross-agency advisory group consisting of state and local representatives was established to work collaboratively through policy, process, and project issues and priorities.

The IJIS Broker acts as a data sharing hub, exchanging information electronically between systems throughout the criminal justice enterprise, regardless of the source or the physical location of the information. Stakeholders involved include Department of Justice (DOJ), law enforcement agencies, prosecutors, district and limited jurisdiction courts, and the Department of Corrections (DOC). Due to their level of involvement and available resources, the DOJ was designated as the managing organization for the IJIS Broker project. Figure 1 depicts the partner agencies, with their associated systems, that make up the web of data exchanges through IJIS Broker. The dotted line indicates that the exchange between the county/city attorneys' case management system and IJIS Broker has not yet been established.

Figure 1
IJIS Broker and Exchange Partners



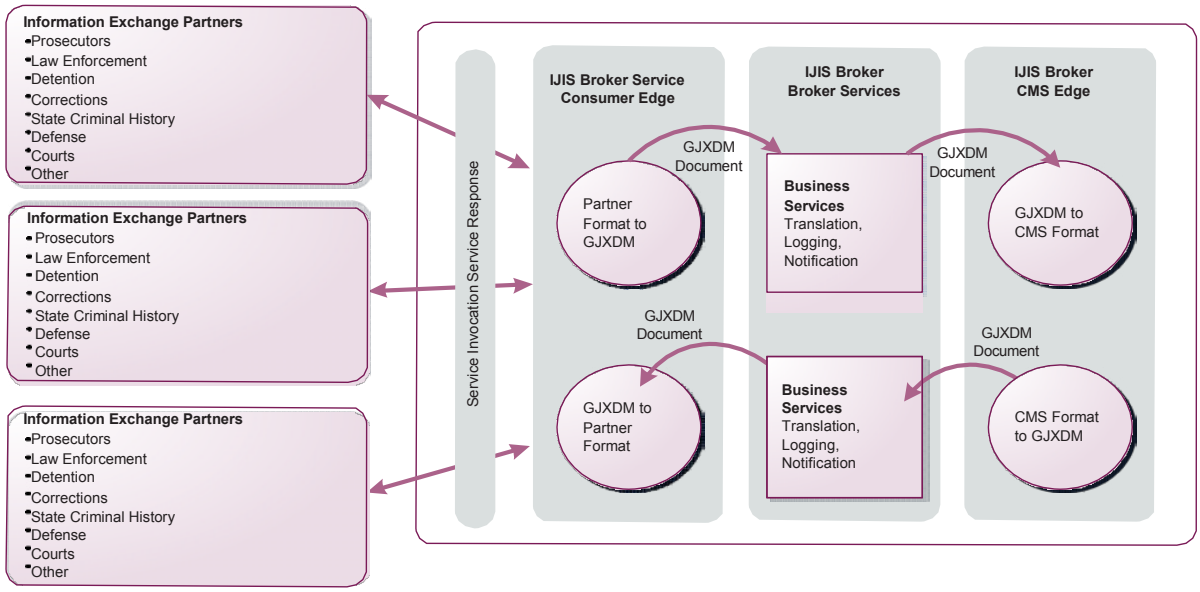
Source: Compiled by the Legislative Audit Division.

From the point of arrest and booking through incarceration and discharge, the data of an offender is shared among different justice agencies. The IJIS Broker helps ensure that this information is entered into the central repository for computerized criminal records, known as Computerized Criminal History (CCH). A criminal record includes most personally identifiable information such as name, age,

sex, race, height, and weight. In addition, records contain criminal justice information such as charges filed and subsequent findings. After receiving the Statewide Automated Victim Information and Notification grant in 2005, DOJ envisioned the IJIS Broker as an integral tool for the creation of a Crime Victims Notification (CVN) application that would allow victims the opportunity to be informed of their offenders' pre-disposition and correction activities, referred to as "current status."

One of the base principles of the IJIS Broker project is to capture justice information once, at the point of origin, and re-use this information whenever possible. The IJIS Broker is able to accomplish this by transforming partner data into a common language that allows for translation, and then reformatting to allow other partners to receive this data. Extensible Markup Language (XML) is highly recognized as a programming language for interchange of data over the internet. Unlike another internet programming markup language known as Hypertext Markup Language (HTML) that deals with appearance of documents and forms, XML specifies what information is contained by using tags to identify information categories. For example, name, eye color, and height would be tagged for personal descriptors, whereas marital status and occupation are tagged for social descriptors. The national standards used by the IJIS Broker for specific justice data categories and formatting are the Global Justice XML Data Model (GJXDM) and the National Information Exchange Model (NIEM). Figure 2 (see page 3) helps illustrate the exchange partners involved, and the role of the IJIS Broker to extract the data from partner system format using GJXDM, log the transaction, and translate into a format for a case management system or recipient partner.

Figure 2
Functionality of IJIS Broker



Source: Department of Justice.

Audit Scope and Objectives

The scope of the audit encompassed the information shared via the IJIS Broker between the following agencies and their respective information systems: the Judicial Branch including District Courts and Courts of Limited Jurisdiction, the Department of Corrections, Department of Justice, and law enforcement. As the project lead for the IJIS Broker system, any recommendations or conclusions are directed towards the Department of Justice. Audit work focused on examining operational enterprise data exchanges and transactions in both calendar years 2015 and 2016. The original project plan (NCHIP 2005) for IJIS Broker includes the following exchanges:

- Arrest Booking Exchange
- Notice of Charges Filed
- Notice of Hearing/Hearing Results
- Court Orders
- Sentencing Recommendation Exchange – OMIS initiated
- Pre-Sentence Investigation Report Exchange
- Correctional Status Exchange
- Law Enforcement Query

The four objectives of the audit are as follows:

1. Evaluate the effectiveness of existing controls that ensure the integrity of the information exchanged by way of the IJIS Broker.
2. Determine whether dispositions within the courts case management system are matched to driver and criminal history through the IJIS Broker in an accurate and timely manner.
3. Examine measures used to provide necessary confidentiality of information shared using the IJIS Broker and verify compliance with federal and state requirements.
4. Evaluate the effectiveness of the IJIS Broker disaster-recovery processes and procedures.

Methodology

The following is a general overview of the procedures followed in order to reach the objectives of the audit:

- Reviewed the IJIS Broker transaction logs.
- Observed the functionality of the IJIS Broker administrative console.
- Reviewed notifications sent from IJIS Broker to partners indicating acknowledgement or error when information is passed.
- Reviewed logs maintained by the Criminal Justice Information Network.
- Tested a sample size of IJIS Broker transactions to verify data integrity.
- Inquired about disposition matching percentage rate between courts and the DOJ.
- Examined the results of a batch file transfer between FullCourt and IJIS Broker.
- Reviewed the administrative access list for IJIS Broker.
- Surveyed the physical security of IJIS Broker and supporting network hardware.
- Inquired about software and hardware configurations used for system, service, and network-level security.
- Observed IJIS Broker disaster-recovery capabilities and supporting documentation.
- Reviewed agency policies and procedures, along with applicable statute and federal regulations.
- Reviewed previous Federal Bureau of Investigation audit report.
- Interviewed staff with the Justice Information Technology Services Division (JITSD) and supporting contractor, along with other exchange partners including DOC, Office of Court Administrator (OCA), Montana Highway Patrol, Missoula municipal court, Missoula city attorney, and Lewis and Clark County clerk of court.

Audit Criteria

In addition to statute and policy (enterprise-wide and agency), the resources used as audit criteria (best practices) throughout the course of fieldwork were the Federal Information System Audit Control Manual from the Government Accountability Office and publications from the National Institute of Standards and Technology (NIST), specifically 800-53 regarding security and privacy controls of federal systems. The Department of Administration uses NIST as a basis for many state information technology (IT) policies and standards within the Montana Operations Manual. In addition, the audited agency provided Microsoft Operational Framework as its template for its own IT governance policies. All of the above documents are generally accepted industry standards from reputable organizations. Regulations specific to criminal justice information, such as Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy, were also referenced for criteria purposes.

Audit Summary

Basic communication infrastructure for the IJIS Broker is in place, with some data exchanges operating successfully. However, the IJIS Broker has yet to reach the full potential of what it was designed to accomplish. Some IJIS Broker enterprise exchanges have not been implemented, and consequently crime victim notification is inoperable at this time. The most crucial of these exchanges is between the courts and the DOJ, which is dependent upon the completion of the FullCourt Enterprise project by the OCA. In addition, business processes from exchange partners, outside the realm of the IJIS Broker, can adversely affect the timeliness of when information is shared, which ultimately effects the point-in-time accuracy of the data. A synopsis for each objective is provided below.

- **Objective 1:** The existing IJIS Broker controls including transaction logs, response transactions, and change management procedures implemented by DOJ provide assurance that the integrity of the data exchanged is not compromised by the IJIS Broker.
- **Objective 2:** Driving dispositions are accurately matched to a driver's record in a timely fashion based on the interface between the computer-aided dispatch application, the IJIS Broker, and the Driver Control System; however, computerized criminal history has factors that limit the effectiveness of information exchange through IJIS Broker and compromise the validity of its data.
- **Objective 3:** The automated controls built into the IJIS Broker, as well as the physical security controls around the network equipment, ensure confidentiality of the data exchanged; however, there are certain business process controls that should be reexamined and strengthened to minimize risk factors for unauthorized disclosure of criminal justice information or personally identifiable information.

- **Objective 4:** DOJ has redundancy built into IJIS Broker from an application, database, storage, and load-balancing perspective; however, facility continuity of operations (COOP) capabilities must be further developed and processes better defined to ensure immediate recoverability of services in the case of a disaster.

Chapter II – Integrity of Data Exchanged via IJIS Broker

Introduction

The Integrated Justice Information Sharing (IJIS) Broker concept is simple by nature, but rather complex by design. As explained in Chapter I, the purpose of the exchange platform is to act as an intermediary hub that receives information from one justice information system, then translates and transforms into a language and format that can be shared and automatically processed by several other justice systems. Since the IJIS Broker does manipulate the data in order to perform the exchange, it was necessary to verify proper controls were in place to ensure that information is not altered during the process. For the first audit objective, the subject areas examined were information system logs, error or acknowledgement responses, incoming and outgoing IJIS Broker transactions, and change control.

Logging of Exchanges/Transactions

It is common practice for information technology (IT) professionals to monitor the use and operational status of their respective information systems or networks. For the first objective, we examined how the Department of Justice (DOJ) monitors the IJIS Broker. With regard to user access to the IJIS Broker, there are few individuals that have access and it would be incorrect to classify them as "users." These individuals are for the most part database administrators, being that the IJIS Broker is not a user-based system. The IJIS Broker works in the background, with criminal justice practitioners accessing their own information systems. However, there are external exchange partners with access to a log that monitors their respective data exchanges, known as the IJIS Broker Transaction Log (IBTL). The log is a web-based service that can be accessed via secure internet connection, specifically for segregated justice partners. For instance, the Office of the Court Administrator (OCA) has an account within IBTL in order to monitor and verify the nightly batch file transfers between the central court repository for its case management system and IJIS Broker. In the case that a transaction is unsuccessful, an error message is logged within the IBTL and a response is sent to the originator. Manual processes are required to correct any identified errors and ensure information is properly collected. All successful transactions are also preserved within IBTL for internal audit purposes.

Response Transactions

Responses are sent from IJIS Broker following a message query or data exchange to inform the originator on whether the transaction was successful. An example of this would be a message indicating that an error occurred due to parameters not entered for

a vehicle registration query from a highway patrol officer console. This query message response would be considered a solicited transaction, meaning there was a request for information sent. Other triggering events can lead to unsolicited transactions, such as correctional status updates within the Department of Correction's Offender Management Information System (OMIS). These messages are sent to the state's central repository for criminal records, known as Computerized Criminal History, when the status of an offender within a state correctional facility has changed. If an error occurred during this transaction, a response would be generated and sent back to OMIS for correction. In addition to error responses, acknowledgement that a transaction was received successfully can also be sent to the originator. During fieldwork, we examined transactions with error responses to better understand the cause. We determined that from the minimal error responses logged in IBTL, the majority were message queries that resulted from human error (i.e. missing information or data being entered incorrectly). Also from this we were able to confirm the IJIS Broker was sending transaction responses on a systematic basis.

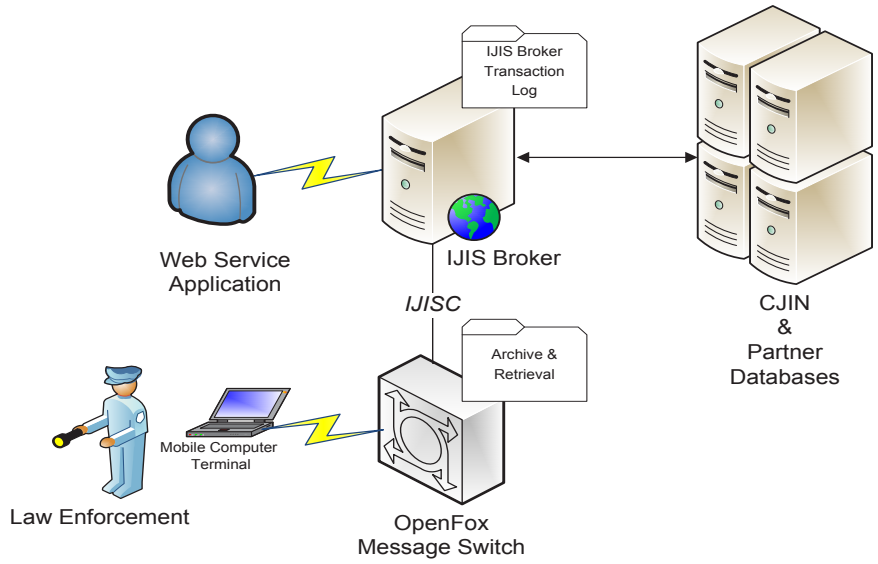
Data Exchange Integrity

A significant amount of traffic travels over the interface between IJIS Broker and the message switch that handles all external message queries and subsequent responses from the Criminal Justice Information Network (CJIN) and other partner databases. Referred to as OpenFox, this software-based message switch receives, stores, and forwards message queries to the proper CJIN system, while also handling the return messages to the originator. To further explain, message queries consist of two to five character abbreviations called message keys. Most, but not all, message keys are used for requesting information from either the state's CJIN, the National Law Enforcement Telecommunications System (NLETS), or the National Crime Information Center (NCIC). The CJIN message keys query the state justice and motor vehicle databases. The NLETS is a network that links all states and many federal agencies. NLETS queries will access this national network to obtain criminal and driving history from outside the state. The NCIC network is an additional resource for criminal data and is managed by the Federal Bureau of Investigation. The NCIC queries will access a national index of theft reports, warrants, and other federal justice information. Between CJIN, NLETS, and NCIC there are almost 200 message keys.

The program manager for CJIN uses the log for the OpenFox message switch, referred to as Archive and Retrieval (A&R), as a tool to perform internal audits and to conduct misuse investigations, such as cases where queries have been made into driver or criminal history for improper or unethical purposes. In one year there were in excess of 28 million transactions over CJIN. There are two different interfaces between OpenFox and IJIS Broker, referred to as "IJISC" and "IJISN." IJISN is designated for

missing persons queries. IJISC is used for all other transactions and was the primary interface where sample messages were taken and compared to IBTL. Figure 3 depicts the relationship between IJIS Broker and OpenFox message switch.

Figure 3
IJIS Broker and OpenFox Message Switch



Source: Compiled by the Legislative Audit Division.

For the purposes of testing the data integrity of the IJIS Broker, we compared incoming and outgoing transactions recorded within IBTL to those recorded in A&R. A random seven days were selected from the previous 12 months of log data across fiscal year 2015 and fiscal year 2016. From these dates, a sample of the transactions were taken from A&R and IBTL for comparison. In order to cover a wide array of messages for testing, we took a percentage of each message key that was used for a given day's sample. Some message keys are used more than others. For instance, "DQ" is the key for driver's license query, which is very likely the most used message key for all law enforcement. Regardless, we did not want our daily random sample to consist of just DQ message keys. Thus, each day's message traffic was broken into the different message keys used, and a percentage was taken from each. Not only was each query message traced and compared from OpenFox to IJIS Broker, but also the corresponding response from IJIS Broker to the requestor through OpenFox. Each individual message was opened and saved to file for comparison. Spreadsheets were created of both law enforcement query messages as well as the nonsolicited IJIS Broker exchanges, such as correctional status and correctional intake transactions from the DOC. These transactions with

IJIS Broker occur based on a triggering event, such as a when an inmate has been paroled or has moved to a different correctional facility.

After all transaction samples were taken and recorded, we compared the information that entered OpenFox message switch to what information was passed to IJIS Broker. Subsequently, if there was a response message, we also compared the information that CJIN provided to IJIS Broker to the information that was passed by IJIS Broker to the requesting entity through the message switch. From our review of the IJIS Broker transactions, there were no instances discovered where the data was inadvertently altered during the exchange (translation and transformation). However, the accuracy of the data as well as the timeliness of the exchange depend greatly upon the controls and business processes of the partner information systems, and will be discussed in Chapter III.

Configuration Change Control

Configuration management is a control category included within the baseline security controls maintained by all state agencies for their information systems, per state policy. Within this category, change control procedures are required to ensure that all changes performed on the IJIS Broker are approved, documented, and tested before notifying stakeholders and implementing the change. Proper change control processes also provide assurance that the data contained, or in this case transported, will not be changed due to modifications made to the system itself. The DOJ did provide its IT governance template, based on a well-respected industry model, which includes configuration management. Using the model, the agency developed its own Operations Framework Change Management Standard Operating Process. In addition to receiving a copy of this policy for review, the audit team examined the SharePoint site that is used as the agency's change management system. A change management system is defined within the change management process as a system used to track the progress of change requests from submission through review, approval, implementation, and closure. Included on the SharePoint site is a spreadsheet used as the change control log with the following fields: ID number, status, due date, scheduled start date/time, title, affected system(s), change manager, creation timestamp, implementation results, description, change type, reason, customer impact, item type, and file path. Every week, the Change Advisory Board (CAB) conducts a virtual meeting to discuss the change control log and current change requests requiring approval. The CAB consists of members from the agency including the system owner, Chief Information Officer, Application Services Bureau Chief, Systems Support Bureau Chief, and Information Security Officer. At times, an extended CAB will be invited which includes a representative from each Information Technology Services Division section of DOJ as determined by the bureau chiefs. We attended this meeting for audit purposes. During

this meeting, the Applications Services Bureau Chief discusses all system changes occurring in the next seven days. Each change request form is shared for discussion and questions are addressed to the requestor, who is also referred to as the change manager. At the end, the Applications Bureau Chief approves or denies the change based on the conversation and any concerns from members of the board. From the evidence gathered, we determined that DOJ has policy and procedures in place to ensure controls are implemented for IJIS Broker change management.

CONCLUSION

The controls implemented by the Department of Justice provide assurance that the IJIS Broker does not compromise the integrity of the data during the exchange between the partner systems.

Chapter III – Accuracy of Records and Timeliness of Data Exchanges

Introduction

When driving or criminal offenses are adjudicated in the courts, the final decision (or disposition) rendered by the judge or jury must be applied to the correct record, which for the purpose of this report is referred to as disposition matching. In addition, dispositions should be added to records in a timely fashion so that law enforcement has the most accurate and up-to-date information available. A driving record is defined under Title 61 of the Montana Code Annotated, while a criminal record is defined under Title 45. The driving and criminal records for citizens of Montana are maintained by the Department of Justice (DOJ) within the Justice Court Reporting System (JCRS) and Computerized Criminal History (CCH), both of which are part of the Criminal Justice Information Network (CJIN). Driving dispositions are not maintained within CCH, thus any driving disposition handed down in district court will not be sent via electronic disposition (e-disposition) and will need to be entered manually into the JCRS. Typically, district courts do not hear traffic violations, so this has not been a challenge for the agency. Coincidently, the courts of limited jurisdiction (COLJ) with e-disposition capability cannot submit criminal dispositions electronically, and these too must be entered into CCH manually. Later in this chapter, other challenges that require manual intervention with criminal disposition matching will be addressed.

Driver Disposition Matching Through IJIS Broker

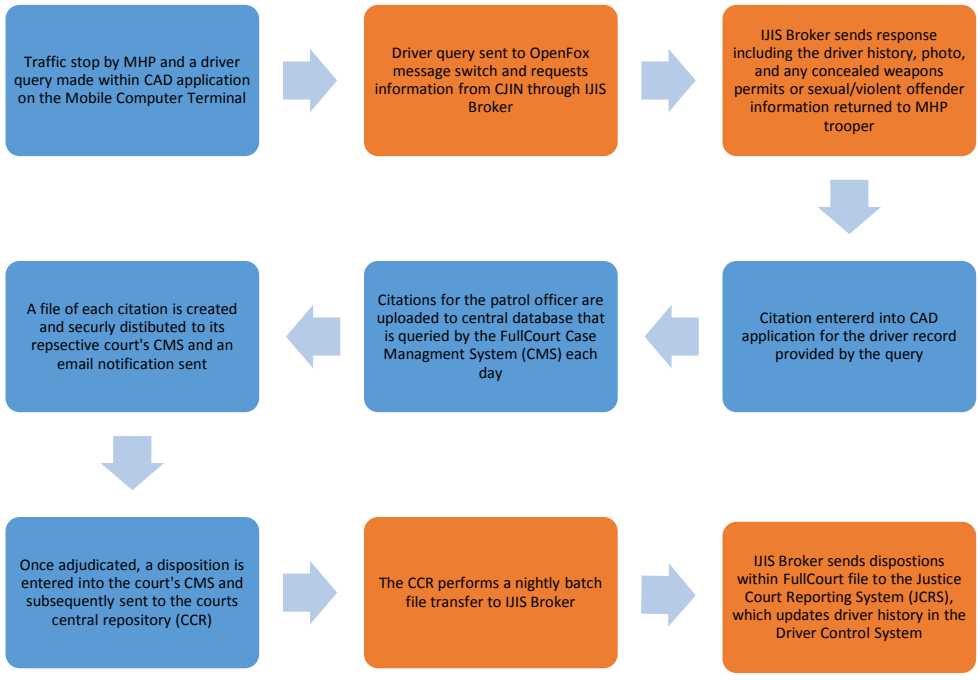
Based on statistics provided at the end of 2016, there are approximately 799,389 registered drivers in Montana. The magnitude of driver records far exceeds that of criminal records, hence the importance of establishing an Integrated Justice Information Sharing (IJIS) Broker exchange that can share and update these records in a timely and accurate manner. During the initial planning stages of our audit work, the 12 most populous courts were reporting driving dispositions electronically for approximately 42 percent of the total driving dispositions in the state. Since that time, two additional courts have come online for a total of 14 courts of limited jurisdiction with electronic reporting, which is estimated at 48 percent of the total dispositions. The remaining 52 percent come from the 120 courts that are still submitting dispositions by hard-copy. The OCA explains that the rate at which courts are moved to electronic reporting depends on the funding provided, which is typically through federal grants. Between 2007 and 2015, the priority to move the remaining courts to electronic reporting moved down the list with other projects needing to be implemented.

During the course of a traffic stop, the patrol officer will obtain the driver's license and registration from the motorist. The officer will then run the license through the computer-aided dispatch (CAD) application on the mobile computer terminal within the patrol car. CAD has card-reader technology with the application that allows the officer to simply swipe the driver's license. There is also the option of typing in the driver's name or license number. The CAD application will then submit a driver query (DQ) to IJIS Broker, which will pull driver history from the Driver Control System (DCS) and a photo from the driver's license photo repository. In addition, each driver query triggers the IJIS Broker to run an additional concealed weapons query and sexual/violent offender query to provide to the patrol officer. A vehicle registration query (RQ) can also be run in CAD, which will again trigger the IJIS Broker to obtain the registration information from the Montana Enhanced Registration and Licensing Information Network (MERLIN).

Observation of Law Enforcement Interface With IJIS Broker

The process between when a driving violation is issued to a motorist by law enforcement and a final disposition being processed and saved to a driver's record is illustrated in Figure 4. The blocks in orange indicate a step that involves the IJIS Broker, whereas the blue indicates involvement of systems outside of IJIS Broker.

Figure 4
The Process From Driving Citation to Disposition



Source: Compiled by the Legislative Audit Division based on interviews with personnel from the Office of Court Administrator.

In order to observe the interoperability of the CAD application and IJIS Broker, contact was made with the Montana Highway Patrol to schedule times to ride along with patrol officers. An auditor accompanied three patrol officers on two separate occasions during their patrol shifts. For each traffic stop that was made, the CAD console was able to access the IJIS Broker and obtain information in less than a few seconds. Each query that was made was noted in order to refer back to within the IJIS Broker Transaction Log and the Criminal Justice Information Network log, Archive and Retrieval. If a driving citation needed to be issued, the CAD application automatically applied the driver information that was queried from the Driver Control System via IJIS Broker to the ticket. Once the ticket is entered, it is stored and later transferred to the case management system for the courts of limited jurisdiction. As stated earlier, all driving dispositions are eventually stored within Justice Court Reporting System.

Due to the real-time interface between the CAD application and the Driver Control System via IJIS Broker, driving citations can be issued with accurate driver information, which reduces the likelihood of dispositions being improperly applied to a driver's record within Justice Court Reporting System. The DOJ indicated the remote possibility that a driver's name change could be accepted by the courts but not by the Motor Vehicle Division, leading to a mismatch with a driving disposition. The probability of this occurring is small, and no examples were identified during any of the times we accompanied the Montana Highway Patrol. A more likely scenario for a mismatch would be that the card reader was either not used or unavailable and the driver's name was typed incorrectly into the CAD application. Once again, there were no recorded instances of this occurring during examination.

Manual Processes Necessary for Criminal Records

A criminal record must begin with a biometric. A biometric is defined as a biological trait that is used as a unique identifier of an individual. For instance, fingerprints, palm prints, retina/iris patterns, and DNA can all be described as biometrics used for identification of criminals. In the state of Montana, fingerprints are the most common biometric used for criminal records. After an arrest, an offender is booked at a city/county detention center where his or her fingerprints are taken. These prints can be captured on a hard copy fingerprint card and mailed to DOJ, or in the case a detention center has access to a LiveScan unit, the criminal can be electronically fingerprinted and submitted instantaneously to the Automated Biometric Identification System (ABIS). ABIS is a criminal biometric database shared among seven western states. As reported by DOJ, approximately 41 LiveScan units are deployed throughout the state, comprising 87 percent of all the arrest/booking transactions. Once a fingerprint is captured and entered into ABIS, a state identification number is assigned by CCH and used as the key identifier for criminal records. These identification numbers are

maintained with their respective biometric in CCH, which includes only Montana criminal records.

Fingerprint Cards and Manual Data Entry

The arrest/booking transaction is an IJIS Broker enterprise exchange that was examined for our first objective of the audit. These transactions are generated from CCH and are essentially email notifications sent to subscribers, such as city/county prosecutors, when an offender has been arrested and booked in a jail within their jurisdiction. A subscriber can be any representative from a justice agency, or a crime victim who requests notification when the status of their offender has changed. The arrest/booking transaction is closely tied to the correctional intake or correctional event transaction. A correctional intake transaction is triggered from the processing of a fingerprint card, via hard copy or LiveScan submittal. After further examination of the correctional intake transactions, the date and time of some of the exchanges did not match the indicated date of the arrest or intake. From our initial sample of only eight offenders and their corresponding CCH correctional intake/event transactions with IJIS Broker, there were two examples where the date of intake was almost two years prior to the fingerprint being processed for that correctional cycle. Most other correctional intake transactions occur within a couple of days of the triggering activity. The explanation provided by DOJ for this date discrepancy could be one of two likely scenarios. Both included the fact that the fingerprints were likely submitted to DOJ using a hard-copy fingerprint card that was either not mailed or was received but needed to be resubmitted due to poor quality. In order to verify these were hard-copy fingerprint cards, DOJ was able to provide additional data within CCH for these given transactions which did show the use of a scanner, indicating the fingerprints were provided on a hard-copy card and scanned into ABIS. The origin for both of the correctional intake transaction examples that were delayed was the Montana State Prison during a correctional cycle. The importance of this detail is that if an offender is moved to the state prison, and the fingerprint is what triggers a notification from CCH through IJIS Broker, there could be a significant delay if the fingerprint is sent through mail. Hard-copy fingerprint cards compromise the timeliness of exchanges through IJIS Broker.

IJIS Broker is also dependent upon manual data entry by partners within the justice community for the timeliness of the data exchanged. We identified another circumstance during fieldwork where a date discrepancy, similar to correctional intake, was uncovered with the correctional status exchange. A correctional status exchange is triggered when there is a change to an offender's status within the Offender Management Information System (OMIS). This could equate to a simple change in correctional facility, or something more significant such as the release of an offender. The cause for the window of time between when the correctional status change

occurred and when the information was passed through IJIS could not be readily explained by DOJ or DOC personnel, but speculation was that it was the result of human error regarding data entry. The capability of the IJIS Broker depends on both exchange partner systems and their associated practices.

Conclusion

Reliance on manual processes such as the use of hard-copy fingerprint cards compromise the accuracy of computerized criminal history, which is accessed by IJIS Broker, based on risk factors associated with timeliness and human error.

Criminal Disposition Matching

Continuing with the criminal justice process, after an offender has been arrested, booked, and detained, the local prosecutor is notified through the arrest/booking transaction. Charges are filed against the offender which must be adjudicated in court. If found guilty, dispositions are handed down. These are then matched to the criminal record that began with the offender's fingerprint. The current configuration of the Court's case management system, called FullCourt, is that each court within the state has its own segregated application of FullCourt. The goal of the Office of the Court Administrator (OCA) is to migrate to an enterprise solution for FullCourt throughout the state. The purpose of this endeavor would not only be to increase consistency with data entry for all courts, but also to implement a more timely exchange between FullCourt and CCH. There are two central court repositories located in Helena that collect data from FullCourt for the courts that have electronic reporting. From these central repositories, there is a batch file transfer each evening to the IJIS Broker. The files are then transferred to CCH. At this time, there are only two district courts with electronic reporting–Lewis & Clark and Missoula in the 1st and 4th Judicial Districts. The progress of the IJIS Broker project was stalled after complications arose with FullCourt exchanges from these two district courts. One such complication is the fact that dispositions cannot be automatically matched to a criminal record. To further explain, within CCH all charges are associated with an arrest. Each arrest is given a number, referred to as a MANS number. In order to amend a specific charge applied to a MANS number, there needs to be individual identifiers for each charge under that arrest. Currently, this does not exist within CCH, so each disposition handed down by the court must be applied to the criminal record manually. According to §44-5-213, MCA, "…dispositions resulting from formal proceedings in a court having jurisdiction in a criminal action against an individual who has been photographed and fingerprinted under §44-5-202, MCA, shall be reported to the originating agency and the state repository within 15 days." Depending on the workload for the Criminal

Records section at DOJ, there is the likelihood that the 15-day deadline will not be met.

DOJ and OCA recognize these circumstances as limiting factors to the timeliness and accuracy of criminal history. This is especially crucial to law enforcement officers who rely on accurate information when dealing with individuals with criminal records, or external parties who do criminal background checks for employment. Both DOJ and OCA are working toward a solution through the development of separate projects. The OCA is planning an enterprise solution for FullCourt, while DOJ will complete an upgrade to CCH. Combined, both will create an arrest tracking number (ATN) as well as a charge tracking number (CTN). The ATN would replace the MANS number, while the CTN would include both the arrest and all the charges associated. Through a user portal, the CTN will be entered and all previous charges/revocations (i.e. historical data) can then be provided for updating. The two projects are heavily funded through federal grants awarded on an annual basis. Over $4 million is estimated for the completion of both projects, with $561,000 of that total requested from the state's general fund. The original estimate for completion on the CCH project was 6 months, which has now been pushed to 8 months. The estimated date of completion is May 31, 2017. For the FullCourt Enterprise project, the original estimate was 17 months for completion, which has been changed in the Legislative Finance Committee report to 24 months (August 16, 2017). While the Department of Justice can make the necessary changes to CCH, a prerequisite for the timely exchange of court data will be completion of FullCourt Enterprise.

RECOMMENDATION #1

We recommend the Department of Justice automate criminal disposition matching between FullCourt and the Computerized Criminal History.

Additional Data Exchanges With FullCourt

There are also plans for additional enterprise exchanges with FullCourt. For instance, a protection order issued by a judge and entered into the court's case management system cannot be sent through nightly batch file transfer with IJIS Broker. Crime victim notification (CVN), which was a large driver for the Statewide Automated Victim Information and Notification grant awarded to DOJ, has been shelved for the time being due to this and the other technical limitations with FullCourt exchanges. No-contact orders and bench warrants are also not shared through IJIS Broker. During the first iteration of trying to resolve these issues, the project ran out of grant money

and CVN was de-prioritized. Other avenues were pursued for crime victim safety. The DOC allocated resources towards Victim Information Notification Everyday (VINE), which is a victim notification service through a third-party vendor, and the DOJ developed the Hope Card system. The Hope Card system is a home-grown solution by DOJ and is managed by the Office of Victim Services (OVS). Victims with permanent orders of protection in place can register with OVS to receive a Hope Card. The card is approximately the size of a driver's license, and includes protection order information (petitioner and respondent) along with a picture of the respondent (offender). The Hope Card uses IJIS Broker to pull the protection order from a CCH "hot file." The hot file is a mirror file of the respondent's criminal history with all nonpertinent sensitive information removed. Protection orders are maintained within the CCH hot file. The photo of the respondent is pulled from the MVD driver's license photo repository, Morpho Trust. The card is easier to carry than the protection order and has reportedly proven beneficial for adolescents in school. In the case an offender is in the vicinity of the victim, information can be provided to law enforcement within any jurisdiction without delay. There have also been efforts to partner with the tribal courts and implement the Hope Card on the reservations. The process has been an added control for verifying that protection orders are included in CCH. On occasion, the Hope Card program manager does not locate the protection order in CCH hot file and has to confirm with the court that issued the order. Nonetheless, the Hope Card system will only provide a level of protection for those who do apply with OVS. In addition, VINE only notifies victims on status of offenders within the state correctional facilities. There are obvious gaps that would need to be filled in order to provide crime victims notification on offenders throughout the entire justice process. CVN did have this vision in mind, but the desired end state is still a work in progress.

RECOMMENDATION #2

We recommend the Department of Justice complete the development and implementation of data exchanges through the IJIS Broker that will share protection orders, no-contact orders, arrest warrants, and bench warrants between FullCourt and the Computerized Criminal History.

Chapter IV – Data Security

Introduction

Data security and confidentiality play a role in all state agencies. However, they play an even more critical role in agencies that handle highly sensitive information, such as criminal justice information (CJI). The FBI's Criminal Justice Information Services (CJIS) Security Policy defines CJI as "…data necessary for law enforcement and civil agencies to perform their mission including, but not limited to biometric, identity history, biographic, property, and case/incident history data." The intent of security policies is to ensure the protection of CJI until the information is released to the public through authorized dissemination, such as the court system. The policy is in place to also ensure any CJI is properly purged or destroyed in accordance with record retention regulations. With the Integrated Justice Information Sharing (IJIS) Broker being a system used primarily for passing CJI between justice entities, much thought and foresight must go into confidentiality when developing the enterprise exchanges. For the purpose of this audit objective, we inquired about both administrative responsibilities regarding data security and the built-in security controls at the service, operating system, and network levels.

Security Management Program

A security management program is essentially a combination of documentation, procedures, tools and techniques that specifically address information security for the information and information systems that support the operations and assets of the organization, including those that are provided or managed by another organization, contractor, or other source. The Department of Justice (DOJ) is currently working from an agency security policy that is in place and expanding this into a more extensive security management plan for the organization. This plan will be a living document that will constantly be changed/edited according to the replacement of old technology with new emerging capabilities. Despite not being able to provide a finalized security program plan, the agency is aware of the importance of data security and has implemented certain features of a security program within the organization. Examples include information security policies, fingerprint-based background checks for personnel (government and contractor), security training, and use of security addenda. DOJ is also audited by the Federal Bureau of Investigation on these controls at a minimum of every 3 years, with the next commencing in June of 2017.

The Montana Operation Manual (MOM) policy regarding information security programs references two separate National Institute of Standards and Technology (NIST) publications as guidance for the state agencies. The first outlines risk management framework and the second addresses the different security control families

(which includes Risk Assessment). Risk management, as defined by NIST, encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. The most integral of the three is the risk assessment, which identifies and evaluates risks and their impacts to the organization. These risk assessments, when encompassed within an agency-wide risk management program, allows the organization to effectively allocate limited resources, both financial and personnel, towards risks that pose the greatest threat to the most critical systems.

IJIS Broker Risk Assessment

While it is almost impossible to eliminate all risk to organizations using information systems to conduct business processes, it is extremely beneficial for DOJ to understand what systems present the most risk and how to mitigate risk to the systems that are the most essential to operations. An agency's information system security program, which includes risk management, is overseen by the Information System Security Officer (ISSO). The ISSO works closely with the system owners on facilitating the risk assessments, since they are best conducted by individuals who understand the mission and business processes. From discussions with the ISSO and the IJIS Broker system owner, it was explained that the agency originally did not have a risk assessment policy in place. In recent years, a policy along with a template for completing the risk assessment was drafted and approved. However, to date a risk assessment has yet to be completed on IJIS Broker. The plans conveyed by the agency provide a rough estimate of when assessments will be completed, but without any scheduled date for IJIS Broker. A system as complex as IJIS Broker, considering the interfaces and the information passed, lends itself to having a substantial amount of inherent risk. Risk assessments are also required by state policy to be completed on an annual basis, along with any updates when significant changes to information systems or environment of operation occur. A report is then written that takes into account any threats, vulnerabilities, likelihood, and impact to the organization operations or assets. In addition, any risk from external parties (i.e. contractors or outsourcing entities) would also be documented. Without routine risk assessments being completed, it is hard for management to prioritize risk mitigation efforts and properly allocate limited resources, specifically time and funding.

RECOMMENDATION #3

We recommend the Department of Justice prioritize and complete a risk assessment of the IJIS Broker and conduct follow-on assessments on a routine basis throughout the entire system development life cycle of the IJIS Broker, including evaluation of both current and future exchanges.

IJIS Broker Communications Protection

As stated above, the second NIST publication from the MOM policy on security programs discusses the security control families along with recommended baselines. Every topic covered under this audit report falls within one of these families of security controls. The following will primarily target the system and communications protection category.

Operating System Level Security

For the purpose of this report, the operating system level security refers to steps taken by the agency to ensure the IJIS Broker servers are protected from threats (internal or external). The IJIS Broker is unlike most information systems in that there is no "user" access per se. Of course, administrators and developers of the IJIS Broker have access to the servers for operations and maintenance. The administrative console is an interface that allows these technicians to monitor and manage messages and enterprise exchanges that pass through the IJIS Broker. Exchange partners are granted auditor access to the IJIS Broker Transaction Log (IBTL) for the purpose of tracking exchanges. The information is limited, though, to only that which pertains to their respective information system. For instance, the information technology manager for the OCA has an auditor account within IBTL to monitor FullCourt exchanges with IJIS Broker. Contractor support plays an essential role in keeping the IJIS Broker operating. However, the obligations of the contract require that only one individual be assigned for on-location support. This contractor does have full administrative access to the IJIS Broker and works closely with the DOJ staff. From our review, full access to the IJIS Broker is limited to key personnel within DOJ and the one contractor.

In addition, common security protocols for remote client access to host servers via unencrypted channels (i.e. internet) are also employed in order to securely transport files. Often referred to as secure shell (SSH), authentication of both the server and the client system is accomplished under this protocol using public key cryptography. For more active clients, such as law enforcement agencies, a virtual private network (VPN) is established. A VPN tunnel is similar to SSH, and both are examples of just one layer of security built in to the IJIS Broker.

Service Level Security

In addition to the secure host connection described above, additional encryption is applied to the data being passed between systems over the Internet. This level of encryption is similar to the connections established for online banking. Referred to as secure sockets layer (SSL), this encryption typically works hand-in-hand with SSH. Also within the service level, authorization is verified. Authorization determines whether a remote client can access certain resources residing on the host server.

Authorization occurs after authentication. To simplify, authentication allows a system to connect to a server, while authorization allows a given user of this system to access a service provided by that server. Authorization can be verified internally or from an external source such as the state's mainframe, active directory, or an Oracle database based on the request from the client.

Another service provided through IJIS Broker is simple mail transfer protocol (SMTP), an Internet standard for email transmission. We identified issues with the use of SMTP messages as part of the examination of arrest/booking transactions that were mentioned earlier in this report. These notifications are generated from CCH and sent by the IJIS Broker to subscribers, typically city attorneys or court administrators, via SMTP. Depending on the information being sent, this may pose no issue as far as confidentiality. However, from our review, some of the emails that are sent do include CJI and personally identifiable information. SMTP is not encrypted, and hence is not a secure means of passing information. While the number of subscribers for these notifications was low, certain individuals were no longer in a position to receive these emails. It was apparent that a review of these subscriptions had not occurred in some time. According to DOJ, the notifications were supposed to be turned off since CVN is currently inactive. As a result, the agency has corrected this issue and notifications are no longer being sent to the subscribers. Nonetheless, the agency should explore other solutions for sending these notifications in the future in the case CVN comes back online.

RECOMMENDATION #4

We recommend the Department of Justice:

A. *Suspend all notification subscriptions receiving criminal justice information through unencrypted channels,*

B. *Develop methodology for verifying notification subscribers on a routine basis, and*

C. *Implement alternate means for sending notifications containing criminal justice information and personally identifiable information that ensures confidentiality.*

Network Level Security

At the network level we inquired about the perimeter security of the agency's network, specifically the firewall configurations. This is an added layer of security between the externally-facing applications and the internal DOJ network. Only certain systems and services in the network allow access by the IJIS Broker, and these can be examined

through the firewall port settings. The use of firewalls and proxies establishes what is referred to as a demilitarized zone (DMZ) for the network, where external applications such as Hope Card/CVN are verified by the proxy as valid traffic and allowed to pass through. None of the back-end services are exposed, creating a logical DMZ.

The default port settings for the DOJ network firewall were provided in the Technical Environment Definition document for the IJIS Broker project, and these were compared to the Access Control List (ACL) that was provided and explained by a DOJ technician. A port in a firewall is essentially an avenue to gain access to a network. Certain ports allow for certain services, and these may be open or closed based on whether that service will be provided by the network to IJIS Broker clients. For instance, we discussed SSH and SSL in the above section. SSH connection for authentication is accomplished through port 22, while SSL encrypted communication occurs through port 443. Both of these ports would need to be open and allow for incoming and outgoing requests on the access control list for the IJIS Broker clients in order to perform SSH and SSL.

In addition, processes related to the firewall configurations were reviewed. For instance, in order to make a change to the network firewall to allow a client access to the network, a firewall change request must be submitted, then reviewed and approved by the DOJ Information Security Office. Also, any new VPN tunnels, as mentioned above, would require approval through an access request form as well as a change to the firewall settings to allow connection. These are submitted to the Justice Information Technology Services Division (JITSD) service desk. We reviewed a sample of requests for both access and changes to the firewall settings.

Physical Security

The final aspect of data security that was examined was physical security of the network and IJIS Broker equipment. For this objective, we conducted a site visit to the Fort Harrison server room, also referred to the Armed Forces Reserve Center (AFRC). Located on the National Guard base, there is secure space allocated to the DOJ for network equipment. The server room is located on the second floor next to the Montana Highway Patrol dispatch center, which is manned 24 hours a day, 7 days a week. Outside the door to the server room is a cipher lock box that holds the key to the door for access. Any visitor must be escorted and sign the visitor log inside the server room. The individual server racks are also locked inside the room. A list of individuals allowed access to the room is maintained by DOJ. There were no indications that physical security of the network equipment and servers is ineffective.

Chapter V – Availability and Disaster Recovery

Introduction

For the last audit objective, we wanted to ensure that the Integrated Justice Information Sharing (IJIS) Broker has a high availability percentage for the justice community due to the critical nature of the information that is exchanged, especially information required by law enforcement. The availability benchmark provided by the agency as a requirement for Criminal Justice Information Services (CJIS) message response is three-nines, which equates to 99.9 percent of the time the IJIS Broker is up and operational. In addition to availability, it is necessary to inspect disaster-recovery capabilities in the case that a natural disaster disrupts service for an extended amount of time. The US DOJ CJIS Security Policy states that agencies must, "…ensure that during intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operation can be eventually reinstituted in a timely and organized manner."

Availability of Service

The IJIS Broker was designed to have redundancy at multiple layers–the application, the database, and for storage. The agency has integrated an active-active model for dual application and database servers, as well as two storage area network (SAN) controllers that have access to the same discs for storage capability. With this design model, regular maintenance can be accomplished by essentially deactivating a server or SAN and performing the patch or update, then doing the same for the other without compromising service to the customer or client. Also, having an active-active configuration for the application servers, this allows a content load-balancer to be implemented. The content load-balancer distributes the traffic load equally among both servers, and in the case that one server should go down the other is already active and can take over. The initial design suggested using clustering for the application servers, which is an active-passive model. The Department of Justice (DOJ) determined early that this method was not as robust as its current configuration.

IJIS Broker Information Systems Contingency Plan

With regards to disaster recovery, we first inquired about a continuity of operations plan (COOP) for the agency or a disaster recovery plan for IJIS Broker which would support the COOP. A COOP focuses on procedures for the overall continuity of the agency's business processes during a disaster. The agency was able to produce a draft of the IJIS Broker Information System Contingency Plan (ISCP). The ISCP is in line with what policy classifies as a Continuity of Support/IT Contingency Plan, which

provides procedures and capabilities for recovering a major application or general support system. The ISCP focuses on IJIS Broker and takes a three-phased approach. The first phase is activation of the ISCP and notification to system owners and users for any outage longer than what is authorized within the plan. The second phase encompasses the procedures for technicians in the recovery of IJIS Broker. The third phase includes testing and validating that the system is back online and functioning as intended. While the ISCP does present a methodical approach for the recovery of IJIS Broker, the document procedures do not include any guidance regarding situations that render the Armed Forces Reserve Center (AFRC) facility unusable. The ISCP does not make any mention of an organizational COOP in the case of a disaster. Instead, it instructs the reader to refer to the AFRC disaster-recovery plan for recovery of services at a separate location. According to National Institute of Standards and Technology (NIST) standards, contingency planning not only involves activities that are required to sustain and recover critical IT services following an emergency, but also pertains to continuity of operations for the department that is affected. If deemed necessary, the ISCP should document necessary arrangements for alternate data processing, storage, and telecommunications facilities. An AFRC disaster-recovery plan was not provided by the agency, but an explanation of the current capabilities along with future plans for IJIS Broker disaster recovery was discussed during interviews and will be addressed in the following section. However, the ISCP does need to fully address the possibility of losing communication connectivity at the AFRC, along with any other single points of failure which may significantly hinder operations supported by the IJIS Broker. Any documented course of action to remedy such a scenario should also be tested on a routine basis to ensure that critical information systems are not rendered inoperable for any extended amount of time. At the time of the audit, the agency had not yet finalized or tested the ISCP.

RECOMMENDATION #5

We recommend the Department of Justice finalize, test, and implement the Information Systems Contingency Plan for IJIS Broker, as well as ensure that the plan is aligned with the organizational Continuity of Operations Plan.

Current and Desired Disaster Recovery Capabilities

Disaster recovery is provided primarily through an enterprise-wide backup software called CommVault. This solution consists of automated backups that are captured and copied to online disc storage, then an additional auxiliary copy procedure is performed by taking the verified backup and writing to an encrypted tape library. The tapes are

retrieved every afternoon at the AFRC and moved to a secure vault on the Capitol complex. In the case a disaster occurs, these tapes are taken to an off-site location and the restored in order to rebuild the entire IJIS Broker environment. The off-site disaster recovery location is in Missoula at a dedicated space for DOJ network equipment with all security and environmental requirements (power and cooling capabilities). A concern of DOJ personnel is the time required for the agency's current disaster recovery solution. The estimate provided by the agency for the time it would take to recover the tapes and completely rebuild the environment at the separate location was approximately 72 hours. While conducting interviews, we were informed of a lightning storm that occurred in June of 2013. A lightning strike hit the AFRC building and caused the cooling system to go off-line, which destroyed some core network equipment. During this instance, the agency restored the cooling and ordered new equipment. While it was not necessary to move to the off-site location, critical services were impaired for almost 8 hours. This can extremely detrimental for law enforcement on duty who rely heavily on CJIN services. In 1984, there was a case where a three-minute Federal Bureau of Investigation (FBI) system outage was a factor in the death of a Missoula Sheriff's deputy. Loss of communication, by even the smallest of windows, can cost the life of either a law enforcement officer or a civilian.

With time being of the upmost importance during any IJIS Broker outage, DOJ has made plans for improving its disaster recovery solution, in accordance with its COOP for complete loss of the AFRC. With the implementation of new technology, the desired end-state is to develop the off-site disaster recovery location into a "warm" site, with equipment in place ready to be activated during a disaster at the AFRC, similar to the incident in 2013. DOJ would essentially replicate services at this site using virtual computing technology and stand-by database management applications, along with purchasing additional servers.

The use of the current alternate location as a COOP site in Missoula is a viable option due to the fact that DOJ already has a presence in the building and a secure network link with the FBI in place. This new IJIS Broker disaster recovery and agency COOP capability is in the planning phase with coordination being done with the State Information Technology Services Division (SITSD). While the potential for the agency to use one of the state's data centers as an alternate location has been presented and not ruled out, the DOJ is exempt from complying with the executive order from the Governor implementing the state information technology convergence plan. This convergence plan requires executive branch agencies to fully share enterprise infrastructure by consolidating network equipment at the state data center by the end of 2017.

RECOMMENDATION #6

We recommend the Department of Justice develop an alternate location with functionality to support critical Integrated Justice Information Sharing Broker applications and processes according to business requirements in the case of a disaster resulting in loss of communication with the Armed Forces Reserve Center.

Department of Justice

Department Response

ATTORNEY GENERAL
STATE OF MONTANA

Tim Fox
Attorney General

Department of Justice
Joseph P. Mazurek Justice Bldg.
215 North Sanders
P.O. Box 201401
Helena, MT 59620-1401

April 17, 2017

Mr. Angus Maciver
Legislative Auditor
Room 160
State Capitol Building
P.O. Box 201705
Helena, MT 59620-1705

Re: *Integrated Justice Information Sharing (IJIS) Broker (15DP-05)* (response to your letter dated March 17, 2017)

Dear Mr. Maciver:

Thank you for your March 17, 2017 letter and for the opportunity to respond to the Legislative Audit Division's March 2017, Department of Justice, Information System (IS) audit titled, *Integrated Justice Information Sharing (IJIS) Broker (15DP-05).*

I will address each audit recommendation in turn.

Recommendation # 1. The Department of Justice (DOJ) automate criminal disposition matching between the FullCourt and Computerized Criminal History.

Concur. The Department of Justice (DOJ), Department of Corrections (DOC), and the Supreme Court (SC) are actively involved in system modernization projects. These projects will result in a direct benefit to information sharing and data matching between the three agencies.

The SC was awarded the National Criminal History Improvement Program (NCHIP) 2014 grant provided by the Federal Department of Justice, Bureau of Justice Assistance, and is using those funds to implement FullCourt Enterprise. Currently there are multiple, non-standardized databases around the state and this project will consolidate them into a single enterprise database with improved technologies, standards, and processes that allows for enhanced data exchanges. FullCourt Enterprise will be implemented in four pilot courts starting in August of 2017.

The DOC is enhancing their Offender Management Information System (OMIS) using funding from the NCHIP 2016 grant. This project will reduce the amount of correctional data silos and provide better information sharing between DOC and DOJ. Anticipated project completion is March of 2018.

The DOJ is modernizing the Computerized Criminal History (CCH) system using funding awarded through the 2015 and 2016 NCHIP grants. These enhancements will eliminate the manual Montana Arrest Numbering System (MANS) process and provide the ability to electronically interface with additional criminal justice agencies. The data exchange between DOJ and the SC will be replaced in the FullCourt Enterprise Data Exchange (FEDEx) project funded with 2015 House Bill 10 appropriations. Standards and processes developed in 2009 will be updated and new data sharing technologies will be implemented with a focus on the immediate need for court order data. The DOJ anticipates project completion in March of 2019.

Recommendation # 2. DOJ complete the development and implementation of data exchanges through the IJIS Broker that will share protection orders, no-contact orders, arrest warrants, and bench warrants between FullCourt and the Computerized Criminal History.

Concur. The Department of Justice and the Supreme Court are actively working to upgrade the existing court data exchange. The protection order, no-contact order, and warrant exchanges will require additional funding and will be included in a future grant requests and as other funding becomes available. Implementation date is not known as there are funding and external project dependencies.

Recommendation # 3. DOJ prioritize and complete a risk assessment of the IJIS Broker and conduct follow-on assessments on a routine basis throughout the entire system development life cycle of the IJIS Broker, including evaluation of both current and future exchanges.

Concur. DOJ is currently finalizing a draft risk assessment with a completion date of 30 June 2017.

Recommendation # 4A. DOJ suspend all notification subscriptions receiving criminal justice information through unencrypted channels.

Concur and Implemented. All email notifications containing Criminal Justice Information have been suspended.

Recommendation # 4B. DOJ develop methodology for verifying notification subscribers on a routine basis.

Concur. The new Connect Montana and Montana Public Safety Information System (MPSIS) will have the ability to verify all users of the system in through automation. Additionally, management of Connect Montana users will be delegated to law enforcement agencies which will allow for a more streamlined user addition and removal process. The DOJ anticipates project completion in March of 2019.

Recommendation # 4C. ***DOJ implement alternate means for sending notifications containing criminal justice information and personally identifiable information that ensures confidentiality.***

Concur. A number of system requirements have been developed for the Connect Montana application that will allow for secure encrypted access to a notification dashboard. Email traffic related to these notifications will only be non-confidential summary information. The DOJ anticipates project completion in March of 2019.

Recommendation # 5. ***DOJ finalize, test, and implement the Information Systems Contingency Plan (ISCP) for IJIS Broker, as well as ensure that the plan is aligned with the organizational Continuity of Operations Plan.***

Concur. DOJ is currently finalizing a draft ISCP. As part of the plan, there is equipment that was planned to be purchased six months ago, however, there was no purchasing contract in place. This issue has just been resolved and a purchasing contract is now available. Once the equipment is purchase and ISCP are finalized, the ISCP process and procedures will be tested. Completion date is expected to be 30 October 2017.

Recommendation # 6. ***DOJ develop an alternate location with functionality to support critical Integrated Justice Information Sharing Broker applications and processes according to business requirements in the case of a disaster resulting in the loss of communication with the Armed Forces Reserve Center.***

Concur. As stated in the response to recommendation #5, we will purchase equipment and pilot an alternate location in accordance with the ISCP. Completion date is expected to be 30 October 2017.

I have included only #1 - #6 of the seven audit reports sent to DOJ. Dawn Temple (#7) did not receive the audit. If you have any questions, please feel free to contact Mike Milburn at 444-4145.

Sincerely,

TIM FOX
Attorney General